Handreichung zum Prüfbogen

Detailpunkte zu Schwerpunkten der Ransomware-Präventionsprüfung

Hinweis: Diese checklistenartige Auflistung stellt wesentliche Elemente zu den untersuchten Prüfungsschwerpunkten dar. Diese Handreichung ist nicht als Antwortbogen zu verstehen und muss daher auch nicht dem BayLDA ausgefüllt vorgelegt werden. Vielmehr soll diese Handreichung die Aussagen, die auf dem Prüfbogen dargestellt werden, näher erläutern und als Hilfestellung dienen. Es handelt sich um Basisanforderungen - nicht jede gelistete Maßnahme ist zwingend erforderlich, sofern andere Maßnahmen ein gleichwertiges Schutzniveau schaffen.

1. Systemlandschaft

☐ Vollständige und aktuelle Liste aller vorhandenen PCs und Notebooks samt Betriebssystem und Betriebssystemversion vorhanden
Grund: Voraussetzung für wirksames Patch Management

☐ Vollständige und aktuelle Liste aller internen und externen Server samt Betriebssystem und Betriebssystemversion vorhanden
Grund: Voraussetzung für wirksames Patch Management

☐ Vollständige und aktuelle Liste aller dienstlichen Smartphones, Tablets und sonstigen mobilen Endgeräte samt Betriebssystem und Betriebssystemversion vorhanden
Grund: Voraussetzung für wirksames Patch Management

☐ Vollständiger und aktueller Netzwerkplan mit allen intern sowie extern betriebenen IT-Systemen samt aktiver und passiver Netzkomponenten (z. B. Switches, Firewalls, VPN-Appliances) samt ggf. vorhandener Netzsegmentierung vorhanden
Grund: Voraussetzung für wirksames Patch Management

☐ Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt
Grund: Soll das Ausbreiten von Schadcode bzw. von Angreifern innerhalb des Netzwerks erschweren/verhindern (sog. Lateral Movement)

☐ Über das Internet erreichbare Server wie Mailserver, Webserver oder VPN-Endpunkte befinden sich in einem eigenen internen Netzsegment und sind dabei mittels einer Firewall vor dem internen Netzwerk abgesichert (sog. Demilitarisierte Zone - DMZ)
Grund: Soll verhindern, dass Angreifer die ggf. kurzzeitig einen derartigen Dienst übernehmen, nicht mühelos auf weitere interne Systeme zugreifen oder zumindest einen Angriffsversuch durchführen können

☐ Anbindung mobiler Arbeitsplätze (z. B. dienstliche Notebooks, dienstliche Smartphones) über das Internet erfolgt über verschlüsselte und auch kryptographisch authentifizierte Verbindungen (z. B. verschlüsselte VPN mit Authentifizierung mittels starken Passwörtern und kryptographischen Client-Zertifikaten)
Grund: Angreifer sollen nicht alleine anhand entwendeter Benutzernamen/Passwörtern ins Unternehmensnetz gelangen können

☐ Aus dem Internet geladene Programme können nicht ohne Nutzerinteraktion ausgeführt werden.
Grund: Verhinderung der automatisierten Ausführung von aus dem Internet nachgeladenen Schadcodeprogrammen, nachdem unbeabsichtigt ein Office-Makro aktiviert wurde

☐ Programme ohne valide Signierung der Authentizität durch das Betriebssystem können nicht ausgeführt werden
Grund: Vom Benutzer fälschlicherweise selbst aus dem Internet heruntergeladene Schadsoftware wird nicht zur Ausführung gebracht

☐ Es werden keine Privatgeräte im Homeoffice vollständig an das Unternehmensnetz angebunden - Empfehlung: ausschließlich dienstlich administrierte Endgeräte verwenden
Grund: Das Schutzniveau privater Endgeräte kann vom Verantwortlichen nicht gewährleistet werden

☐ Dienstliche Smartphones und Tablets werden über eine Mobile-Device-Management-Lösung verwaltet
Grund: Voraussetzung für wirksames Patch-Management sowie Datenlöschung im Verlustfall

☐ Die Installation von Software auf einem PC ist nur mittels Admin-Rechten (durch den Administrator) möglich
Grund: Verhinderung, dass Nutzer aus Versehen als normale Software getarnten Schadcode installiert

☐ Browser-Plugins (z. B: Flash, Java) werden nur dann installiert, wenn eine (ältere) Anwendung dies unbedingt erforderlich macht
Grund: Viele Browser-Plugins besitzen Sicherheitslücken, die schon beim Besuch einer Webseite ausgenutzt werden können (sog. Drive-By-Angriff)

☐ Skripte wie JavaScript oder Visual Basic werden nur dann vom Betriebssystem (nicht vom Browser, hier ist zumindest JavaScript in der Regel erforderlich) ausführbar gelassen, wenn (ältere) Software dies unbedingt erfordert
Grund: Manche Schadsoftware kommt als Skript-Datei im E-Mail-Anhang und kann durch Deaktivierung auf Betriebssystemseite bei einem versehentlichen Klick durch den Nutzer trotzdem an der Ausführung gehindert werden

☐ Microsoft-Office-Pakete sollten so konfiguriert werden, dass diese nur signierte Makros ausführen
Grund: Schadsoftware kommt häufig in Form präparierter Office-Dokumente wie Word oder Excel. Diese besitzen keine signierten Makros und können so an einer Ausführung gehindert werden.

☐ Prüfung, ob die Ausführung von Programmen nur aus festgelegten Verzeichnissen (sog. Execution Directory Whitelisting) möglich ist
Grund: Präparierte E-Mails enthalten häufig nicht den Schadcode selbst, sondern kleine Programme, die diesen automatisch aus dem Internet laden. Die derart heruntergeladenen Schadprogramme werden in festgelegten Verzeichnissen des Betriebssystems gespeichert und können durch eine Freigabe gültiger – und in diesem Fall anderer – Verzeichnisse an einer Ausführung gehindert werden.

☐ Auf dem E-Mail-Server wird ein Spam- und Antivirenfilter eingesetzt
Grund: Damit können schon bekannte Schadprogramme erkannt und verdächtige E-Mails gesondert behandelt werden

☐ E-Mails mit gefährlichen Dateianhängen wie ausführbaren Dateien, mit Passwort verschlüsselten ZIP-Archiven oder Office-Dokumente mit Makros werden vom Mailserver in einen Quarantäne-Ordner zur Analyse verschoben
Grund: Derartige E-Mails enthalten häufig Schadcode bzw. kleine Programme, die Schadcode herunterladen sollen. Da diese mittlerweile nicht häufig sind, kann eine manuelle Analyse durch die IT-Administration gut durchgeführt werden.

☐ Der E-Mail-Server wird so konfiguriert, dass E-Mails von internen Absendern, die aber von außerhalb des Unternehmens zugestellt werden sollen, blockiert werden (sog. Anti-Spoofing)
Grund: Dieser Angriff ist nicht unüblich, um Beschäftigte bspw. zum Klick auf einen in der E-Mail enthaltenen Link (der zu Schadcode führt) zu verleiten. Da derartige E-Mails immer von „außerhalb" kommen, kann es faktisch nicht sein (außer ggf. bei E-Mail-Verteilern, dies sollte dann getestet werden), dass diese eine internen Absenderadresse haben und nicht gefälscht sind.

☐ Administratoren besitzen zwei Benutzer-Accounts: Einen für reine Administrationsaufgaben und einen für andere Tätigkeiten wie E-Mails lesen oder im Internet surfen
Grund: Schadcode führt sich immer mit den Benutzerrechten der Person aus, die (versehentlich) zu dessen Aktivierung beigetragen hat. Auf diese Weise kann zumindest verhindert werden, dass der Schadcode gleich mit (lokalen) privilegierten Administrator-Rechten zur Ausführung kommt.

☐ Auf jedem PC/Server wird für das lokale Administrator-/Root-Konto ein unterschiedliches und starkes (mind. 16 Stellen) Passwort verwendet
Grund: Wenn ein Angreifer/Schadcode das lokale Administratorkonto eines Rechners erlangen kann, ist so nicht gleich die Weiterbewegung (sog. Lateral Movement) über das gesamt Netzwerk möglich

2. Patch Management

☐ Alle PCs und Notebooks sind so konfiguriert, dass Softwareupdates des Betriebssystems automatisch eingespielt werden
Grund: Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden

☐ Sofern Softwareupdates des Betriebssystems über eine eigene Softwareverteilung erfolgt (z. B. WSUS), dann ist diese so zu konfigurieren, dass Sicherheitsupdates automatisch vom Hersteller des Betriebssystems geladen und unverzüglich für Updates an alle PCs und Notebooks bereitgestellt werden
Grund: Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden

☐ Es werden ausschließlich Betriebssysteme eingesetzt zu denen der Hersteller Sicherheitsupdates zur Verfügung stellt
Grund: Sicherheitslücken können sonst gar nicht geschlossen werden

☐ Es besteht eine vollständige Liste der auf allen PCs und Notebooks eingesetzten Anwendungssoftware samt Softwarestand
Grund: Voraussetzung um das Einspielen von Softwareupdates organisieren zu können

☐ Anwendungssoftware auf PCs und Notebooks wird so konfiguriert, dass Softwareupdates (zumindest Sicherheitsupdates) automatisch eingespielt werden sofern dies möglich ist
Grund: Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden

☐ Sofern Anwendungsprogramme nicht automatisch aktualisiert werden können, wird sichergestellt, dass diese spätestens monatlich auf den aktuellsten Stand gebracht werden
Grund: Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden

☐ Es werden ausschließlich Server-Betriebssysteme eingesetzt, für die vom Hersteller noch Sicherheits-Updates bereitgestellt werden
Grund: Sicherheitslücken können sonst gar nicht geschlossen werden

☐ Es wird für alle Server geprüft, inwiefern diese so konfiguriert werden können, dass Sicherheitsupdates automatisch eingespielt werden können
Grund: Verhinderung, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im lokalen Netzwerk missbrauchen können

☐ Für alle Server, bei denen keine automatisierte Einspielung von Sicherheitsupdates aufgrund von Risiken möglicherweise instabiler Serverzustände möglich ist, werden Sicherheitsupdates nach Tests unverzüglich manuell eingespielt. Kritische Sicherheitslücken werden innerhalb weniger Tage zur Anwendung gebracht, sofern keine gleichwertigen anderen Schutzmaßnahmen ergriffen werden
Grund: Verhinderung, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im lokalen Netzwerk missbrauchen können

☐ Sicherheitsupdates aller Netzwerkkomponenten, insbesondere Firewalls und VPN-Appliances werden unverzüglich mit hoher Priorität eingespielt
Grund: Insbesondere bei über das Internet erreichbaren, zentralen Systemen bedeutet ein erfolgreicher Angriff einen sofortigen Ausfall kritischer Schutzkomponenten

☐ Es besteht eine aktuelle und vollständige Dokumentation darüber, welche PCs, Notebooks, Server, Netzwerkkomponenten,… automisch oder manuell upgedatet werden. Bei nicht-automatischen Updates werden dabei die jeweiligen IT-Systeme samt Softwareständen erfasst.
Grund: Nur durch eine minimale und schlanke Dokumentation kann auch die Wirksamkeit eines Update-Konzepts sichergestellt und kontrolliert werden

☐ Sicherheitsupdates für dienstliche Smartphones und dienstliche Laptops werden über ein Mobil-Device-Management-System unverzüglich ausgerollt. Es werden keine mobilen Endgeräte eingesetzt, für die es keine Sicherheitsupdates (mehr) gibt.
Grund: Verhinderung, dass Angreifer mittels Ausnutzung bekannter Sicherheitslücken mobile Endgerät erfolgreich angreifen und damit Zugang zum Unternehmensnetz erhalten können

3. Backup-Konzept

☐ Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen (inkl. Originaldaten), 2 verschiedene Backupmedien (auch „Offline" wie Bandsicherungen) und 1 davon an einem externen Standort oder vergleichbar wirksame Backup-Mechanismen bezüglich Ransomware-Angriffen
Grund: Im Falle einer Ransomware-Attacke können die (personenbezogenen) Daten und die betroffenen IT-System wieder hergestellt werden

☐ Mindestens ein Backup-System ist durch Schadcode nicht unmittelbar verschlüsselbar (z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems, Air-Gap-getrennt (offline) nach Abschluss des Backup-Prozesses oder Schreibberechtigung auf Backups nur von festgelegten Programmen aus)
Grund: Viele Ransomware-Angriffe versuchen vor einer Verschlüsselung, die Backupsysteme ebenfalls zu verschlüsseln oder die Backups zu löschen. Durch auf Ransomware-Angriffe ausgerichtete Lösungen sollen Risiken bezügl. aktiver Löschversuche der Backups minimiert werden

☐ Es besteht eine dokumentierte Regelung, welche Daten von welchen Servern oder PCs/Notebooks in ein Backup-Konzept aufgenommen wurden
Grund: Sicherstellung, dass alle relevanten (personenbezogene) Daten auch von einer Backup-Lösung umfasst sind

☐ Es wurde ein Planspiel durchgeführt, wie das komplette IT-System in dem Fall wieder aufgesetzt werden kann, falls alle internen wie externen Server aufgrund einer Vollverschlüsselung nicht mehr funktionsfähig wären
Grund: Vorbereitung auf den Worst-Case, um prüfen zu können, ob auch alle erforderlichen Daten im Backup enthalten sind

☐ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird
Grund: Ein Backup muss täglich durchgeführt werden – es ist auch sicherzustellen, dass dieses funktioniert

☐ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert
Grund: Verhinderung der Situation, dass im Worst-Case festgestellt wird, dass bspw. ein Backup-Medium defekt ist oder für eine Systemwiederherstellung erforderliche Information nicht im Backup enthalten sind

4. Überprüfung des Datenverkehrs

☐ Der zentrale Internetübergangspunkt vom internen Netzwerk zum Internet ist mittels einer Firewall abgesichert
Grund: Mindeststandard zur Absicherung vertraulicher Netze gegenüber dem Internet

☐ Neben/als Bestandteil der Firewall wird http-Verkehr über einen Web-Proxy geleitet. Netzwerkverkehr anderer Protokolle ins Internet wird als Standard von der zentralen Firewall geblockt und nur im Einzelfall dokumentiert freigeschalten
Grund: Voraussetzung für Analyse von möglichem Schadcode-Netzwerkverkehr

☐ Die Web-Proxy-Komponente filtert aufgerufene Internetseiten bezüglich bekannten und täglich aktualisierten Endpunkte, die als (meist gehackte) Server zur Auslieferung von Schadcode verwendet werden (sog. Indicator of Compromise, kurz: IoC) und blockiert sowie protokolliert derartige Aufrufe
Grund: Schadcode wird meistens in mehreren Schritten „ausgeliefert", was mitunter auf diese Art und Weise unterbunden werden kann

☐ Es findet eine Protokollierung des Datenverkehrs ins Internet auf Basis von externen IP-Adressen und Datenvolumen für bis zu 90 Tage mit dem Ziel einer Auswertung möglicher Unregelmäßigkeiten nach einem Vorfall statt. Diese Protokolle sollten verschlüsselt werden, um einen missbräuchliche Verwendung zu verhindern und die datenschutzrechtliche Zweckbindung sicherzustellen.
Grund: Bei dem Verdacht einer Datenausleitung nach einem Ransomware-Angriff kann auf diese Weise eine Indiz geschaffen werden, ob eine Datenausleitung stattgefunden hat oder nicht. Die IP-Adressen können dann der Polizei für deren Ermittlungen ausgehändigt werden

5. Awareness und Berechtigungen

☐ Regelmäßige Schulung der Beschäftigten bezüglich aktueller und häufiger Cyberangriffe (z. B. einmal pro Jahr)
Grund: Kriminelle erschleichen sich durch Social-Engineering-Angriffe wichtige Informationen für nachgelagerte Cyberattacken. Entsprechend ist es wichtig, allen Beschäftigten den „Sicherheitsfaktor Mensch" in geeigneten Schulungen zu erläutern.

☐ Konsequente Einweisung neuer Beschäftigter zum fachgerechten Umgang mit den IT-Komponenten und Verhalten bei Social-Engineering-Angriffen
Grund: Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden

☐ Sensibilisierung neuer Beschäftigter bezüglich IT-Risiken vor der Aufnahme der Datenverarbeitung (z. B. auch bei Aushilfskräften)
Grund: Sicherheitstechnisches Fehlverhalten von Beschäftigten beruht oft auf fehlender Sensibilisierung und Unterrichtung im Vorfeld

☐ Darstellung des Ablaufs von Social-Engineering-Angriffen zur Sensibilisierung der Beschäftigten (z. B. Möglichkeit der Manipulation von Telefonnummern)
Grund: Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden – die Darstellung konkreter Abläufe verbessert das Wissensbild

☐ Informationen an die Mitarbeiter über Meldewege (z. B. durch den ISB oder DSB) und Zuständigkeiten
Grund: Eine angemessene Reaktion auf sicherheitstechnisches Fehlverhalten ist ein entscheidender Faktor für eine wirksame und zeitnahe Reaktion auf einen Cyberangriff